Nortel

Contivity® VPN Client

(Software Version 5.11_021)

FIPS 140-2 Non-Proprietary Security Policy

Level 1 Validation
Version 0.14

December 2004

Table of Contents

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Contivity VPN Client from Nortel. This Security Policy describes how the Contivity VPN Client meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/cryptval.

The Contivity VPN Client is referred to in this document as VPN Client, Client, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Nortel website (http://www.nortel.com) contains information on the full line of products from Nortel.
- The CMVP website (http://csrc.nist.gov/cryptval) contains contact information for answers to technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Nortel. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2

Validation Documentation is proprietary to Nortel and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Nortel.

2. CONTIVITY® VPN CLIENT

2.1 Overview

The Contivity VPN Client provides the user-side functionality for secure remote access over IP networks using Contivity IP access routers and VPN servers. The Contivity VPN Client ensures end-to-end network security by establishing a fully encrypted and authenticated VPN connection from a user's desktop across the Internet, terminating on a Contivity VPN switch located at a trusted enterprise location.

The following table details the security level achieved by the Contivity VPN Client in each of the eleven sections of FIPS 140-2.

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC	3
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

Table 1 – Security Level Per FIPS 140-2 Section

The Contivity VPN Client is a software module composed of a set of binaries running on the Windows 2000 or XP Operating System (OS) on a general-purpose personal computer (PC). In FIPS 140-2 terminology, the Contivity VPN Client is a multi-chip standalone module that meets the level 1 FIPS 140-2 requirements. The module was tested for FIPS 140-2 requirements on Windows XP Professional with Service Pack 2.

Physically, the module is composed of the components of a general purpose PC, and the physical cryptographic boundary is the case of the PC. The PC or motherboard manufacturer could provide a block diagram for the exact hardware on which the module is installed, and the physical cryptographic boundary surrounds all of those components.

Logically, Contivity VPN Client consists of four binaries running on the Windows 2000 or XP Operating System, and the logical cryptographic boundary includes these four components, as depicted in Figure 1.

- CVC Application – Performs IKE and provides a GUI.
- IPSec Driver – Performs IPSec.

- Filter Driver – Filters traffic other than IKE and IPSec communications.
- Library – Interfaces with MSCAPI for authentication using digital certificates.

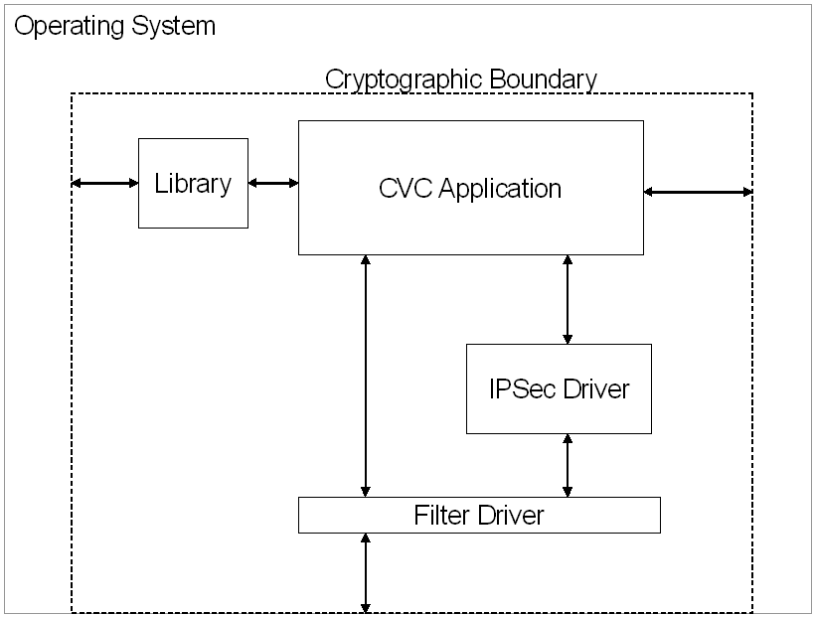

Figure 1 – Logical Block Diagram

2.2 Module Interfaces

The Contivity VPN Client's physical ports are those provided by the general purpose PC, including the Ethernet ports and mouse/keyboard ports. The Client's logical interfaces are composed of graphical user interfaces (GUIs), command line interfaces (CLIs), application programming interfaces (APIs), configuration and log files, and packets traversing the network stack.

A mapping of the FIPS 140-2 logical interfaces to the VPN Client's logical interfaces and the physical ports of the PC can be found in the following table.

FIPS 140-2 Logical Interface	Contivity VPN Client Logical Interface	PC Physical Port
Data Input Interface	The data input is any data sent into the module through the network stack to an application on the PC (such as email, browser, etc), and any data coming into the module through the network stack from the network ports. Also, data input from the module by MSCAPI for certificate processing and RSA operations.	Network ports
Data Output Interface	The data output is any data going out of the module through the network stack from an application on the PC (such as email, browser, etc), and any data going out of the module through the network stack out the network ports. Also, data output from the module to MSCAPI for certificate processing and RSA operations.	Network ports
Control Input Interface	Data read from configuration files, data input via the CVC GUI or command line interface.	Keyboard ports, hard disk, mouse ports
Status Output Interface	The Status Output is all messages either logged by the module or the messages in the GUI. The error messages from IKE negotiations are also status output. The logged informational and error messages can be seen through the log files provided.	Hard disk, monitor ports

Table 2 – Physical Ports and FIPS 140-2 Logical Interfaces

2.3 Roles and Services

There are two roles that operators may assume within the Contivity VPN Client, the Crypto Officer role and the User role. The Crypto Officer is responsible for installation and local configuration of the Client. The User access the module's VPN services.

Operators can be authenticated by the Windows Operating System. Authentication to the Server is performed during IKE using pre-shared keys and digital certificates. However, these authentication mechanisms are not tested on a level 1 FIPS 140-2 validation.

2.3.1 Crypto Officer Role

The Crypto Officer role has the ability to install and configure the Contivity VPN Client. Descriptions of the services available to the Crypto Officer role are provided in the table below.

Service	Description	Input	Output	CSP	CSP Access
Installation	Installing the VPN Client	Command options or	Result of installation	HMAC-SHA1 for Integrity	Read

Service	Description	Input	Output	CSP	CSP Access
		Commands		check	
Client Installation Customization	Client software installation customization using setup.ini				
Create a connection	To configure connection parameters	Command options	Status of command, response and results	Authentication Data	Read/Write
Profile data	Add/Edit/Delete a profile	Command options	Status of command, response and results		
Authentication Options	Authentication to the Contivity Gateway	Command options or Commands	Command response	Authentication Data	Write
Name Server Options	To specify a DNS or WINS server, overriding the Contivity Gateway	Command option			
KeepAlives	To enable or disable KeepAlive packets that maintain a connection during idle periods	Command options	Command response		
Auto Connect	Install/Uninstall Auto Connect feature	Command options	Command response		
Connect before Logon	To enable or disable the Contivity VPN Client GINA dialog box on logon	Command options	Command response		
Uninstall	To uninstall the client software	Command options	Command response		
Start/Stop	Starts/stops the CVC services. The self tests are performed during the module start/restart.	Menu options or Commands	Status of command	HMAC-SHA1 for Integrity check	Read
Show status	Status messages for the module written to log file and Event Viewer.	Commands	Status info in log file		
Zeroization	Zeroizing CSPs	Uninstalling the module and reformatting the hard drive		All	Write

Table 3 – Crypto Officer Services, Descriptions, CSPs

2.3.2 User Role

The User role accesses the module's VPN functionality by initiating an IPSec connection with the Server. The service descriptions and inputs/outputs are listed in the following table:

Service	Description	Input	Output	CSP	CSP Access
VPN session	Use the VPN services within an IPSec tunnel	Encrypted/decrypted data	Encrypt/decrypted data	Session keys	Read/Write
Connect	To establish VPN session by authenticating to the Contivity Gateway	Authentication Information	Result of login attempt	Authentication Data	Read/Write
Edit profile	Edit the profile information on the Client	Command options	Updated profile information	Authentication Data	Read/Write
Change password	Change the current password used on the Contivity Gateway	Current password	Updated password	Password	Write
Monitor Status	To monitor connection status	Command options	Status of command		
Disconnect	To end the VPN session	Command options	Status of command	Session keys	Write

Table 4 – User Services, Descriptions, Inputs and Outputs

2.4 Physical Security

Contivity VPN Client v5.11_021 is a software module and does not implement any physical security mechanisms.

Although Contivity VPN Client v5.11_021 consists entirely of software, the FIPS 140-2 tested platform is a standard PC which has been tested for and meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for home and business use as defined in Subpart B of FCC Part 15.

2.5 Operational Environment

The Contivity VPN Client runs on the general purpose Windows 2000 or XP Operating System, which are considered to be single user mode Operating Systems for FIPS 140-2 compliance. The module was tested on the Windows XP Service Pack 2 operating system.

2.6 Cryptographic Key Management

The Contivity VPN Client implements the following FIPS-approved algorithms:

- AES-CBC (128, 256 bits) – FIPS 197 (certificate #218)
- Triple DES-CBC (168 bits) – FIPS 46-3 (certificate #310)
- SHA-1 – FIPS 180-2 (certificate #299)
- HMAC-SHA1 – FIPS 198 (certificate #28)
- PRNG – General purpose implementation of FIPS 186-2 [(x-Original); (SHA-1)] (certificate #62)

Additionally, the module utilizes the following non-FIPS-approved algorithm implementation in a FIPS mode of operation as allowed by Annex D of FIPS 140-2:

- Diffie-Hellman Group 2 (1024 bit)
- Diffie-Hellman Group 5 (1536 bit)

The following algorithms are disabled within the module in a FIPS mode of operation:

- Diffie_Hellman Group 8 (ECDH)
- Diffie-Hellman Group 1 (768 bit)
- DES
- 40-bit DES
- MD5
- HMAC-MD5

The module supports the following critical security parameters:

Key	Key type/size	Generation	Storage	Use
Integrity check HMAC-SHA1 key	HMAC (160 bits)	Externally generated predetermined value hard-coded into the module	Non-volatile memory (hard drive – plaintext)	Software integrity check
FIPS 186-2 PRNG Seed key	160 bits	Internally generated by gathering system entropy	Not stored – in volatile memory only (plaintext)	Used by FIPS 186-2 PRNG
Passwords (Group and User)	Alphanumeric string (minimum of 6 characters)	Externally created by an operator and entered into the module	Not stored – in volatile memory only; or non-volatile memory (hard drive – plaintext)	Generate pre-shared keys for authentication during IKE
IPSec pre-shared keys	160 bits	Internally generated by hashing user id and password	Not stored – in volatile memory only (plaintext)	Mutual authentication between the module and the server
RSA public keys (Certificates)	RSA public key (1024 bits – 4096 bits)	Externally generated and input into and output from the module during IKE	Not stored – in volatile memory only (plaintext)	Mutual authentication between the module and the server

IKE DH key pair	Diffie Hellman Group 2 (1024 bits) or Group 5 (1536 bits)	Internally generated for use during IKE	Not stored – in volatile memory only (plaintext)	Used for session key agreement – public key sent to server
IKE DH public key	Diffie Hellman Group 2 (1024 bits) or Group 5 (1536 bits)	Externally generated and loaded into the module during IKE	Not stored – in volatile memory only (plaintext)	Used for session key agreement – received from server
IPSec session keys	AES (128, 256 bits) Triple-DES (168 bits), HMAC SHA-1 keys (160 bits)	Negotiated during IKE using Diffie-Hellman key agreement	Not stored – in volatile memory only (plaintext)	Used to encrypt/decrypt/ HMAC tunnel traffic

Table 5 – Listing of Key and Critical Security Parameters

All the keys contained only in volatile memory are not stored in the module and are zeroized immediately after use. All other CSPs can be zeroized by uninstalling the module and reformatting the hard drive.

2.7 Self-Tests

The Contivity VPN Client performs the following self-tests at power-up:

- Software integrity check: Verifying the integrity of the software binaries of the module using an HMAC-SHA1 keyed hash.
- AES Known Answer Test (KAT): Verifying the correct operation of the AES algorithm implementation.
- Triple-DES KAT: Verifying the correct operation of the Triple-DES algorithm implementation.
- SHA-1 KAT: Verifying the correct operation of the SHA-1 algorithm implementation.
- HMAC-SHA1 KAT: Verifying the correct operation of the HMAC-SHA1 algorithm implementation.
- FIPS 186-2 RNG KAT: Verifying the correct operation of the FIPS 186-2 RNG implementation.
- Alternating bypass mode test: Verifying the integrity of the modules bypass capability hardcoded in the filter driver.

The Contivity VPN Client performs the following conditional self-tests:

- FIPS 186-2 Continuous RNG: Verifying that the Approved RNG has not failed to a constant value.

- Continuous RNG for entropy gathering: Verifying that the seed for the FIPS 182-2 PRNG has not failed to a constant value.

The Contivity VPN Client will start its services only after all the self tests have passed. If the self tests have not passed, it enters an error state and logs the failure. All error conditions can be cleared by restarting the module.

2.8 Design Assurance

Nortel follows highly stabilized and popular design procedures. The design goes through many phases of review and inspections, and implementations undergo rigorous quality assurance testing.

Additionally, ClearCase Version 5.0 is used to provide configuration management for the Contivity VPN Client's software and documentation. This software provides access control, versioning, and logging.

2.9 Mitigation of Other Attacks

This section is not applicable. The Contivity VPN Client v5.11_021 does not claim to mitigate any attacks beyond the FIPS 140-2 level 1 requirements for this validation.

3. SECURE OPERATION

The Contivity VPN Client meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

3.1 Crypto Officer Guidance

The Crypto Officer is responsible for installation, customization configuration, management of the module, and removal of the module. More details on how to use the module can be found in Configuring the Contivity VPN Client and Using the Contivity VPN Client in FIPS Mode documents.

3.1.1 Installation

The module performs RSA operations and digital certificate processing using MSCAPI. In a FIPS mode of operation, the module must be installed on a Microsoft Windows 2000 or XP (Home or Professional) Operating System that has a FIPS-validated MSCAPI module. Currently the following versions of MSCAPI are FIPS validated:

FIPS Cert #	Windows platform	rasenh.dll version
238	Windows XP	5.1.2518.0 5.1.2600.1029 [SP1] and 5.1.2600.2161 [SP2]
103	Windows 2000 SPx	5.0.2150.1391 [SP1], 5.0.2195.2228 [SP2] and 5.0.2195.3839 [SP3]
76	Windows 2000	5.0.2150.1

Table 6 – Current FIPS validated MSCAPI and their platforms

The testing was performed on Windows XP Professional SP2 which ran v 5.1.2600.2161 of rsaenh.dll

3.1.2 Management

By default, the Contivity VPN Client v5.11_021 is configured for a FIPS mode of operation. The module can be put in a non-FIPS mode during custom installation or configuration. When switching between FIPS and non-FIPS modes the operator must zeroize the group and user passwords by overwriting them with new values. However, an operator must not perform switching between FIPS and non-FIPS mode when using the module in a FIPS mode of operation.

3.1.3 Zeroization

At the end of the life cycle of the module, the Crypto-Officer must uninstall the module's software and then overwrite all addressable locations with a single character and reformat the hard drive which contained the software. This will zeroize all hard coded keys or CSP's stored within files.

3.2 User Guidance

The User accesses the module's VPN functionality. The User must not modify the configuration of the module as established by the Crypto Officer, nor should a User reveal any of the CSPs (such as group and user passwords) used by the module to other parties.

4. ACRONYMS

API	Application Programming Interface
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DES	Digital Encryption Standard
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
HMAC	(Keyed-) Hash MAC
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security
KAT	Known Answer Test
MAC	Message Authentication Code
MSCAPI	Microsoft Cryptographic API
NIST	National Institute of Standards and Technology
OS	Operating System
PC	Personal Computer
PRNG	Pseudo Random Number
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SA	Security Association
SHA	Secure Hash Algorithm
SP	Service Pack
VPN	Virtual Private Network